IN THE CLAIMS:

Claims 1-19 (Cancelled)

20. (Currently Amended) A method, comprising:

enabling integrity checking of a software module to be used in a mobile communication terminal, said terminal capable of communicating in a mobile communication system, said software module already stored on a removable memory unit connected to the terminal and ready for use except, before allowing the software module to take control of the terminal, the terminal communicates via the mobile communication system with a software provider, said communication including:

hashing the software module on the removable memory unit, resulting in a first hash value,

transmitting by said terminal of identifying information concerning said terminal and said memory unit to said software provider, wherein said transmitting of identifying information comprises transmitting a first identifier, associated with the memory unit, a second identifier, associated with the terminal and the first hash value via the mobile communication system to said software provider,

receiving by said terminal from said software provider a digitally signed data block comprising a reference value for use during integrity checking of said software module, ~~and~~ said data block comprising a digital signature and further data associated with the memory unit and the terminal,

analyzing the received data block, comprising verification of the digital signature and comparison of said further data with said first and second identifiers,

storing the received data block comprising the digital signature, thereby providing a reference value for use during integrity checking of said software module, for allowing the software module to take control of the terminal only if the integrity of the software module properly checks.

21. (Cancelled)

22. (Currently Amended) An apparatus, comprising:

a device for enabling integrity checking of a software module to be used in a mobile communication terminal, said terminal capable of communicating in a mobile communication system, said software module already stored on a removable memory unit connected to the terminal and ready for use except, before allowing the software module to take control of the terminal, the terminal communicates via the mobile communication system with a software provider, said device including:

a device for hashing the software module, resulting in a first hash value, wherein said transmitting of identifying information comprises transmitting a first identifier, associated with the memory unit, a second identifier, associated with the terminal and the first hash value via the mobile communication system to said software provider;

a transmitter for transmitting identifying information concerning said terminal and said memory unit to said software provider; ~~and~~

a device for receiving, from the software provider, a data block comprising a digital signature and further data associated with the memory unit and the terminal;

a device for analyzing the received data block, comprising verification of the digital signature and comparison of said further data with said first and second identifiers; and

a device for storing the received data block comprising the digital signature, thereby providing a reference value for use during integrity checking of said software module for ~~a receiver for receiving a digitally signed data block comprising a reference value for use during integrity checking of said software module and~~ allowing the software module to take control of the terminal only if the integrity of the software module properly checks.

23. (Cancelled)

24. (New) The method of claim 20 wherein said integrity checking comprises:

hashing the software module for providing a second hash value, and

checking whether or not the second hash value matches the first hash value for said allowing the software module to take control of the terminal only if the integrity of the software module properly checks.

25. (New) The apparatus of claim 22 configured to hash the software module and provide a second hash value, to check whether or not the hash value matches the first hash value for said allowing the software module to take control of the terminal only if the integrity of the software module properly checks.